IFW

Attorney's Docket No. 047138/257085

PATENT

AF/2134

In The United States Patent And Trademark Office

Appl. No.: 09/518,583
Applicant(s): Chee-Seng Chow, et al.
Filed: March 3, 2000
Art Unit: 2134
Examiner: Mossadeq Zia
Title: SYSTEM AND METHOD FOR ACCESSING A REMOTE SERVER FROM AN INTRANET WITH A SINGLE SIGN-ON

Confirmation No.: 5843

Docket No.: 047138/257085
Customer No.: 00826

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF TRANSMITTAL
(PATENT APPLICATION – 37 C.F.R. § 41.37)

1. Transmitted herewith is the APPEAL BRIEF in this application, with respect to the Notice of Appeal filed on August 26, 2004.

2. □ Applicant claims small entity status.

3. Pursuant to 37 C.F.R. § 41.20(b)(2), the fee for filing the Appeal Brief is:
   □ small entity $170.00
   ☒ other than small entity$340.00

Appeal Brief fee due $340.00

☒ Any additional fee or refund may be charged to Deposit Account 16-0605.

Respectfully submitted,

Trent A. Kirk
Registration No. 54,223

CUSTOMER NO. 00826
ALSTON & BIRD LLP
Bank of America Plaza
101 South Tryon Street, Suite 4000
Charlotte, NC 28280-4000
Tel Charlotte Office (704) 444-1000
Fax Charlotte Office (704) 444-1111

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Brief-Patent, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on October 6, 2004.

Lorna Morehead

Lorna Morehead

Attorney's Docket No. 047138/257085

PATENT

In The United States Patent And Trademark Office

Appl. No.:	09/518,583	Confirmation No.:	5843
Applicant(s):	Chee-Seng Chow, et al.	Art Unit:	2134
Filed:	March 3, 2000	Examiner:	Mossadeq Zia

Title: SYSTEM AND METHOD FOR ACCESSING A REMOTE SERVER FROM AN INTRANET WITH A SINGLE SIGN-ON

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF UNDER 37 CFR § 1.192

This Appeal Brief is filed pursuant to the "Notice of Appeal to the Board of Patent Appeals and Interferences" filed August 26, 2004.

1. ***Real Party in Interest.***

The real party in interest in this appeal is GetThere, Inc., the assignee of the above-referenced patent application.

2. ***Related Appeals and Interferences.***

There are no related appeals and/or interferences involving this application or its subject matter.

3. ***Status of Claims.***

The present appeal involves Claims 1-22, which are presently under a final rejection as set forth by the Official Action dated May 26, 2004. The claims at issue are set forth in the attached Appendix.

4. ***Status of Amendments.***

No amendments have been filed subsequent to the final Official Action of May 26, 2004.

5. ***Summary of Claimed Subject Matter.***

The present invention provides a method, system, and computer-readable medium for performing multiple user authentications with a single sign-on. As such, a user may be initially authenticated such as upon accessing a first or local server. This initial authentication also serves to authenticate the user as the user accesses a remote sever. In this regard, a token containing authentication information may be passed to the remote server such that the user can be authenticated by the remote server without entering any additional information. According to the present invention, the token also includes information regarding an account for the user including at least one of a new account for the user and an update to an existing account for the user. As such, by simply logging on to the first or local server, an account or user profile is created for the user without the user having to also access or enter information at the remote server. The user profile may store information that may be updated and is useful for providing efficient and individualized service to the user.

Figure 1 illustrates one embodiment in which an Intranet **102** connected to a remote server **104**. In one embodiment, the remote server **104** could be a host travel reservation and booking service. (Page 5, lines 23-25). In order to gain access to the remote server **104**, the user typically logs onto an Intranet server **120** with a username and password. (Page 6, lines 10-17). The user may use the Intranet and resources external to the Intranet once signed on to the Intranet server (Page 7, lines 1-3). According to the present invention, because the Intranet server **120** has already authenticated the user, the user can select a link for the remote server, where the Intranet server **120** sends a token containing authorization information to the remote server **104** causing the remote server to authenticate the user without the user needing to perform a second sign-on. (Page 7, lines 6-11).

Independent Claim 21 includes means-plus-function language. In particular, Claim 21 generally recites means for performing a first user authentication and means for selecting a remote server. The means for performing a first user authentication generally includes a workstation running a browser program that a user accesses through a computer interface having associated software and/or hardware to perform a first user authentication (See Page 7, lines 1-26; Page 9, lines 10-18). The means for selecting a remote server also comprises a workstation operating a browser program from which a user selects a remote server, for example, by clicking a link from a list of links presented on the user's browser (See Page 7, lines 1-5; Page 9, lines 3-9). Claim 21 also recites means for sending a token to the remote server. The means for sending the token is comprised of a network such as the internet, wide are network, local area network, or other computer interface (See Figure 1; Page 5, line 22 – Page 6, line 2; Page 10, lines 23-26). In addition, Claim 21 recites means for decoding the authentication information. The decoding could be performed by transmitting a universal resource locator (URL) with an encrypted token to remote server code along a transmitted URL data path (See Figure 3; Page 10, lines 23-26). As such, the means for decoding the authentication information comprises a remote server operating to decode the authentication information. In one exemplary embodiment, the remote server code could include a CGI module, a remote server application, and an error handler, where the CGI module may decode the URL and decrypt the decrypted token (See Page 10, line 26 – Page 11, line 7). In alternative embodiments, the remote server code may include alternative interface code architectures than the CGI module (See Page 11, lines 8-10).

In one embodiment, the Intranet server **120** sends an encrypted user identification ("user ID") and time stamp to the remote server **104**, where the remote server can decode the user ID and time stamp to authenticate the user. (Page 7, lines 11-15). In addition to the authorization information, the token sent by the Intranet server to the remote server may also advantageously include information regarding an account for the user including at least one of a new account for the user and an update to an existing account for the user. The user is then given access to the remote server **104** and functions available through the remote server. (Page 7, lines 16-17). Since the token also includes information regarding a new account and/or an update to an existing account, the remote server can create and maintain accounts and/or profiles to more efficiently provide service to the user without the user having to also access or enter information at the remote server.

The present invention may be implemented at least partially in software, as shown in Figure 3, in which the Intranet **300** may include a user's browser **308** and Intranet server code **302**. The Intranet server code **302** may include remote server module **304** and an encryption module **306**. When activated, the remote server module **304** may examine the status of the user's authentication access to the Intranet, and if authenticated, the remote server module **304** may respond to a remote link request **312** by providing a URL with an encrypted token **314** to the user's browser for use in accessing remote server code **320**. (Page 9, lines 25 – Page 10, line 5). Once the URL with the encrypted token **314** has been provided, the user's browser **308** may transmit the URL with the encrypted token to the remote server code **320** along URL data path

316 that extends to the remote server. If a remote server application **324** of the remote server code **320** executed by the remote server authenticates the user **324** based on the token, then a welcoming page **318** is sent to the user's browser. (Page 11, lines 11-13). Conversely, if the remote server application **324** cannot authenticate the user, then an error handler **326** of the remote server code **320** generates an error message. (Page 11, lines 18-21). According to the present invention, the token also includes information regarding an account for the user including at least one of a new account for the user and an update to an existing account for the user such that a user account and/or profile may be stored at a remote server to provide efficient service for the user without the user having to also access or enter information at the remote server.

Figure 6 illustrates the contents of an authentication token, which takes the form of a credential token **600** in this particular embodiment. The credential token **600** typically includes a username **602**, an expiration time **604**, and a checksum **606**, where the credential token may be encrypted by the Intranet server and placed into a URL for transmission and subsequent user authentication by the remote server. (Page 13, lines 16-21). The expiration time **604** aids in preventing a user from circumventing the security access features of the remote server, while the checksum **606** may give an indication of data integrity when the credential token **600** is examined by the remote server. (Page 13 line 25 – Page 14, line 23). If the checksum **606** is invalid, an error message is generated, while if the checksum is valid, the expiration time **604** is examined to determine if it is within a selected tolerance. (Page 15, lines 21-25). As explained below, the token also includes information regarding an account for the user including at least one of a new account for the user and an update to an existing account for the user.

With reference to Figure 8, a flowchart is shown which illustrates a method for adding a new user. In step **802**, the user performs an Intranet user authentication process. In decision step **804**, the Intranet server determines whether the user is a new user. If so, the Intranet server sets a new user flag in step **806**. In step **808** the Intranet server forms the fields for the token, including the new user flag, and, in step **810**, the token fields are concatenated to form a single binary string. In step **814**, the binary string is encrypted. Upon the first attempt of the user to access the remote server and the services offered thereby, the token including the information regarding the new user is transmitted to the remote server. The remote server then receives and decrypts the token in step **822** and, if the remote server determines the token is valid, the new user flag status is tested in step **828**. If the new user flag is set and if the remote server software is set to enable adding new users, then in step **834**, the remote server tests to see if the username is already in use. If not, then, in step **838**, a new user account is established, and, in step **840**, the user is authenticated. Thus, this aspect of the present invention facilitates the creation of accounts with multiple servers even though the new user is only required to enter the new account information once.

In addition to or instead of providing information regarding a new user, the token can include information regarding a change or update to an existing account. Referring to Figure 9, for example, a flowchart for a method for updating a user's profile is shown. The user profile information may include information about the user that may help the remote server provide efficient service to the user. (Page 18, lines 8-9). For instance, if the remote server is a travel reservation and booking service, user profile information may include dietary choices, seating preferences, travel spending limits, and other information specific to a given user. (Page 18, lines 9-13). In step **902**, the user performs an Intranet user authentication. In decision step **904**, the Intranet server determines if the user wishes to create a new user profile or update an existing user profile. If so, the Intranet server places the user profile data into strings in step **906**. In step **908**, the Intranet server forms the fields for the token, including the new user profile data and, at step **910**, the token fields are concatenated to form a single binary string. In step **914**, the binary string is encrypted. When the user attempts to access the remote server and the services offered thereby, the token including the information regarding the user profile is transmitted to the remote server. The remote server then receives and decrypts the token in step **922** and, if the remote server determines the token is valid, the token is examined for user profile information in step **928**. If user profile information is found, and if the remote server software is set to enable updating user profile information, then in step **938**, the remote server creates a new user profile or updates any existing user profile. As such, this particular aspect of the present invention allows the user to enter profile information that may be updated and used to provide efficient service for the user without the user having to enter or update the information at multiple remote servers.

As such, the method, system, and computer-readable medium of the present application allow a user to access a remote server from an Intranet utilizing a single sign-on authentication. The present invention eliminates the need for additional sign-on authentication for the user when a user accesses a first server, such as an Intranet server, and wishes to also access remote servers. Thus, the method, system, and computer-readable medium prevent the user from having to remember and enter additional sign-on information, such as a different password, for each remote server, which provides increased security for the user's authentication information.

6. ***Grounds of Rejection to be Reviewed on Appeal.***

(i) Claims 1, 11, 21, and 22 stand rejected under 35 U.S.C. § 102(a), as being anticipated by U.S. Patent No. 5,241,594 to Kung; and

(ii) Claims 2-4, 9, 10, 12 and 13 stand rejected under 35 U.S.C § 103(a) as being unpatentable over U.S. Patent No. 5,241,594 to Kung in view of U.S. Patent No. 5,661,807 to Guski et al. In addition, Claims 5-8 and 15-18 stand rejected under 35 U.S.C § 103(a) as being unpatentable over the Kung '594 patent in view of the Guski '807 patent and further in view of Microsoft Press, Computer Dictionary, 3rd edition (1997).

7. ***Argument.***

(i) Rejection of Claims 1, 11, 21, and 22 under 35 U.S.C. § 102(a) over U.S. Patent No. 5,241,594 to Kung

The Official Action rejects Claims 1, 11, 21, and 22 under 35 U.S.C. § 102(a) as being anticipated by U.S. Patent No. 5,241,594 to Kung ("the Kung '594 patent").

The Kung '594 patent discloses a system and method of authenticating users in a distributed computing system that includes a multiple logon procedure. The user is required to logon to the distributed computing system only a single time and then the user can access all available computers connected to the network via the multiple logon procedure. Generally, the Kung '594 patent discloses storing ID code's and encrypted passwords in a database file at a central server or at respective remote computers within the system. Thus, when a user desires to use a particular remote computer, such as a remote database, for example, a request initiated by the user is processed by the multiple logon procedure which accesses a stored file in the database that contains the user ID code and encrypted password, accesses the remote computer and then automatically enters the user's ID code and password for that computer. In providing the remote computer with the user's information, the multiple logon procedure decrypts the encrypted password for the particular requested computer and logs the user onto that computer using the ID code and decrypted password. (See Col. 2, lines 12-50). The authentication information transmitted in the network (the user ID and password) is protected by using a secure protocol and communication path to prevent others from recording the authentication information for later logon attempts, to prevent others from impersonating another user, and to guarantee the integrity of the authentication information. (See Col. 3, lines 18-24). In operation of a system of the Kung '594 patent, an individual user is assigned a single password for the entire system **10**. After the user successfully logs onto one computer, such as the workstation **11**, the encrypted password is transmitted by a secure transfer protocol **22** to the remote host computer **13** where, if the received ID code and encrypted password matches the ones stored at the remote host computer **13**, the user is automatically logged on. (See Col. 6, lines 3-15 and Figure 1). The Kung '594 patent also states that the invention may be easily configured to work with mainframes and workstations by simply registering a user at the multiple logon server. (See Col. 3, lines 35-37).

In contrast to the Kung '594 patent described above, independent Claims 1, 11, 21 and 22 recite a method, system, and computer readable medium for performing multiple user authentications with a single sign-on by performing a first user authentication, selecting a remote server, and sending a token to the remote server that contains authentication information responsive to the first authentication and information regarding an account for the user including at least one of a new account for the user and an update to an existing account for the user. The authentication information is then decoded to induce a second user authentication.

As defined above, the information regarding a new or updated account that is included in the token of the claimed invention may come in various forms. With respect to the embodiment of Figure 8 of the present application, the token may include fields, including a field for a new user flag that is set when the Intranet server detects a new user. (Page 16, lines 12-15). The embodiment depicted by Figure 9 of the present application adds the capability to transmit new or updated user profile information to the remote server. As described above, the remote server may store user profile information that may help the remote server, such as a travel reservation and book service, provide efficient service to the user (*e.g.*, dietary choices, seating preferences, travel spending limits, *etc.*). Once the token is determined to be valid, the token is examined for user profile information, and the remote server may create an account for a new user or update an account for an existing user depending upon the user profile information. Thus, the multiple user authentication of the claimed invention not only provides a single sign-on procedure, but also provides a capacity for efficiently creating or updating user accounts at the remote server.

While the Kung '594 patent discloses a system and method of authenticating users in a distributed computing system that includes a multiple logon procedure, it does not describe performing multiple user authentications with a single sign-on by sending a token to the remote server that contains authentication information responsive to a first authentication and <u>information regarding an account for the user including at least one of a new account for the user and an update to an existing account for the user</u>, as recited by independent Claims 1, 11, 21, and 22. The Kung '594 patent describes that when a user desires to use a particular computer, such as a remote database, for example, a request initiated by the user is processed by the multiple logon procedure which accesses a stored file that contains the user ID codes and encrypted passwords, accesses the remote computer, and then enters the user's ID code and password for that computer. The multiple logon procedure decrypts the encrypted password for the particular requested computer and logs the user onto that computer using the ID code and decrypted password. Thus, the Kung '594 patent does not describe a token containing information regarding an account for the user including at least one of a new account for the user and an update to an existing account for the user, as recited by independent Claims 1, 11, 21, and 22. In fact, the Kung '594 patent does not describe any technique for creating new accounts or updating accounts with a remote computer.

Although the Kung '594 patent also states that the invention may be easily configured to work with mainframes and workstations by simply registering a user at the multiple logon server (See Col. 3, lines 34-37), this does not describe creating a new user account or updating an existing user account. The Kung '594 patent only states that once a user logs onto the multiple logon server, the user may access other remote hosts, such as mainframes and workstations, because the user ID and password stored on the multiple logon server are used to log the user onto the remote host without further input from the user.

The Official Action finds that "[i]t is irrelevant what the authentication information is since this step does not fundamentally change the process of authenticating a user. Neither does it change how the system operates, nor does it change the computer readable medium having stored instructions." (See page 6, paragraph 21). However, these statements fail to recognize that the information regarding an account for the user is used in the authentication process. As described in the specification of the present application, if the remote server is set to enable a new user, then the remote server tests to see if the username is already in use, and if it is in use, an error message is generated and the user is not authenticated. (Page 17, line 24 – Page 18, line 1). Furthermore, if the username is not in use, a new user account is established and the user is then authenticated. (Page 18, lines 1-4). As such, the information regarding a new account is used in the authentication process, and the user cannot be authenticated until the user is determined to be a new user. Similarly, with respect to information regarding an update to an existing account for the user, if the remote server software is set to enable updating user profile data, the remote server creates a new profile or updates an existing user profile prior to authenticating the user. (See Page 19, line 23 – Page 20, line 2). In this regard, it is also apparent that the information regarding an update to an existing account for the user is used in the authentication process and is not simply "extra data incorporated into the token." Therefore, contrary to the findings in the Official Action, the information regarding an account for the user including at least one of a new account for the user and an update to an existing account for the user may "change the process of authenticating a user," "change how the system operates," and change the computer readable medium having stored instructions."

None of the remaining references, alone or in combination (the combination of which Applicants submit is improper as noted below), teaches or suggests performing multiple user authentications with a single sign-on by sending a token to the remote server that contains authentication information responsive to a first authentication and information regarding an account for the user including at least one of a new account for the user and an update to an existing account for the user. Specifically, U.S. Patent No. 5,661,807 to Guski et al. ("the Guski

'807 patent") discloses an authenticating system that uses one-time passwords. A system **100** of the Guski '807 patent includes a requesting node **102** and an authenticating node **104** interconnected by a communications channel **106**. The requesting node **102**, which is assumed to be a personal computer or workstation, contains a one-time password generator **300**. The requesting node also has memory locations for storing a user ID **302** identifying the user, an application ID **304** identifying the host application being accessed, a signon key **306** used as a key for the encryptions and a time/date value **308**. Values **302-308** provide inputs to the password generator **300**. Thus, the password generator **300** generates a one-time password **310** as a function of the user ID **302**, application ID **304**, signon key **306** and time/date **308**. Password **310** is transmitted to the authenticating node **104**, together with the user ID **302** and application ID **304**, as part of the signon request **320**. The authenticating node **104**, which is assumed to be a host computer, contains a password evaluator **312** that receives the signon key **314** and the signon request **320** from the requesting node **102**. Password evaluator **312** uses these quantities to regenerate the original time/date **308**, which is compared with the reference time/date **316** to determine whether the difference between the two is within a predetermined tolerance. If so, the password evaluator **312** authenticates the user and grants access to the application; otherwise the evaluator denies access. (See Col. 6, line 7 to Col. 7, line 1 and Figure 1).

Each one-time password that is correctly generated includes a particular "signature." The signature is exploited as a performance advantage during the one-time password evaluation process to quickly recognize (before decipherment of the password) 8-character string passwords that cannot possibly be valid one-time passwords and may therefore be trivially rejected. (See Col. 11, lines 40-48). Stated somewhat differently, the translation routine generates a password containing redundancy. Other means such as checksums or the like may also be used to produce an authentication code containing the desired redundancy. (See Col. 11, lines 49-65).

While the Guski '807 patent discloses an authenticating system that uses one-time passwords, the one-time passwords are effective only one time and do not permit multiple user authentications with a single sign-on by sending a token to the remote server that contains authentication information responsive to a first authentication and information regarding an account for the user including at least one of a new account for the user and an update to an existing account for the user, as recited by independent Claims 1, 11, 21, and 22. While the Guski '807 patent states that the password generator **300** generates a one-time password **310** as a function of the user ID **302**, application ID **304**, signon key **306** and time/date **308**, it does not state that the one-time password that is sent to an authenticating node includes any information regarding an account for the user, such as the creation of a new user account or updating of an existing user account, as recited in the claimed invention.

The Microsoft Press, Computer Dictionary, 3rd Edition ("the Microsoft Press reference") states that a flag can be a code, embedded in data, that identifies some condition, or it can be one or more bits set internally by hardware or software to indicate an event of some type, such as an error or the result of comparing two values.

The statements defining a flag in the Microsoft Press reference also do not describe performing multiple user authentications with a single sign-on by sending a token to the remote server that contains authentication information responsive to a first authentication and information regarding an account for the user including at least one of a new account for the user and an update to an existing account for the user, as recited by independent Claims 1, 11, 21, and 22. Although the Microsoft Press reference states that a flag can be a code, embedded in data, that identifies some condition, or it can be one or more bits set internally by hardware or software to indicate an event of some type, such as an error or the result of comparing two values, this does not teach or suggest that a token may contain information regarding an account for the user that includes a new account and/or an update to an existing account for the user, as recited in the claimed invention.

Since none of the cited references teach or suggest a token containing information regarding an account for the user including at least one of a new account for the user and an update to an existing account for the user, Applicants submit that the method, systems, and computer-readable medium of Claims 1, 11, 21, and 22, and their respective dependent claims are not anticipated by any of the cited references, taken either individually or in combination, and that the rejection of Claims 1, 11, 21, and 22 under 35 U.S.C. § 102(a) is overcome.

(ii) Rejection under 35 U.S.C. §103(a) over U.S. Patent No. 5,241,594 to Kung, U.S. Patent No. 5,661,807 to Guski, and Microsoft Press, Computer Dictionary, 3rd Edition

The Official Action also rejects Claims 2-4, 9, 10, 12, and 13 under 35 U.S.C § 103(a) as being unpatentable over the Kung '594 patent in view of the Guski '807 patent. In addition, the Official Action rejects Claims 5-8 and 15-18 under 35 U.S.C § 103(a) as being unpatentable over the Kung '594 patent in view of the Guski '807 patent and further in view of the Microsoft Press reference. Although the Office Action Summary indicates that Claims 1-22 are rejected, the Detailed Action fails to discuss any rejections pertaining to dependent Claims 14, 19, and 20. However, the Applicants assume for purposes of the appeal that all of the claims are rejected.

It is initially submitted that the Kung '594 patent cannot properly be combined with the Guski '807 patent or the Microsoft Press reference. In order to properly combine references, a teaching or motivation to combine the references is essential. *In re Fine*, 337 F.2d 1071, 1075 (Fed. Cir. 1988). In fact, the Court of Appeals for the Federal Circuit has stated that, "[c]ombining prior art references without evidence of such a suggestion, teaching, or motivation simply takes the inventor's disclosure as a blueprint for piecing together the prior art to defeat patentability -- the essence of hindsight." *In re Dembiczak*, 175 F.3d 994 (Fed. Cir. 1999). Although the evidence of a suggestion, teaching, or motivation to combine the references commonly comes from the prior art references themselves, the suggestion, teaching, or motivation can come from the knowledge of one of ordinary skill in the art or the nature of the problem to be solved. *Id.* In any event, the showing must be clear and particular and "[b]road conclusory statements regarding the teaching effect of multiple references, standing alone, are not 'evidence'." *Id.*

In the present application, the requisite motivation or suggestion to combine the Kung '594 patent with the Guski '807 patent or the Microsoft Press reference is lacking. In this regard, the Kung '594 patent is premised on authenticating users in a distributed computing system. The Kung '594 patent provides methods and apparatus that prevent a user from having to separately logon to each computer in the distributed computer system. Conversely, the Guski '807 patent is directed to a system for authenticating a user using a one-time password that changes psuedorandomly with each request for authentication. Thus, each of the Kung '594 patent and the Guski '807 patent is directed to solving a different problem, where the Kung '594 patent is concerned with a one-time logon process to prevent a user from having to separately logon to other computer systems, while the Guski '807 patent is concerned with protecting a password that is used only one time with a password required for each subsequent logon and with the password not being used to gain access to more than one computer. Since the nature of the problem to be solved is different for each patent, the patents cannot be properly combined. Furthermore, the Microsoft Press reference does not teach or suggest authentication, as the reference is cited only for the definition of a "flag," where a flag is typically a code or bits that may identify some condition or event. Moreover, there is no motivation or suggestion to combine the Microsoft Press reference with the Kung '594 patent or Guski '807 patent, as neither patent defines any type of flag. Therefore, there is no teaching or suggestion to combine the Kung '594 patent with either the Guski '807 patent or the Microsoft Press reference.

In any event, even if the references were combined, the claims of the present application are patentably distinct from the cited references, taken either individually or in combination, for at least the same reasons described above with respect to independent Claims 1, 11, 21 and 22. That is, the cited references, even if taken in combination, fail to teach or suggest sending a token to a remote server that contains authentication information responsive to a first authentication and information regarding an account for the user including at least one of a new account for the user and an update to an existing account for the user.

(a) Claims 2 and 12

Furthermore, the combination of the references do not teach or suggest dependent Claims 2, 5-8, 12, and 15-18 rejected in the Official Action. In this regard, dependent Claims 2 and 12 recite that the token is coupled to a universal record locator (URL). The Official Action acknowledges that the Kung '594 patent fails to teach or suggest sending the token within a URL, but cites the Guski '807 patent for the proposition that "the host application" is equivalent to a URL. However, the Guski '807 patent only refers to an authenticating node **104** containing a host application **318**. The user located at a requesting node **102** signs on to gain access to the host application. The password generator **200** generates a one-time password that is transmitted to the authenticating node. A password evaluator **312** determines whether the password may be authenticated and sends a message **322** to the requesting node with its disposition. Nowhere does the Guski '807 patent teach or suggest a token sent within a URL. As known to those skilled in the art, a URL is known generally as the address of a web page on the world wide web. The Guski '807 patent simply describes a password created by the password generator dependent on the user ID, application ID, signon key, and time/date, as well as a message from the password evaluator that may be transmitted by a communications channel. The user is merely attempting to gain access to a host application. Even assuming that the host application could be a URL, a token or any other information, is not being transmitted within the URL, as recited by dependent Claims 2 and 12.

(b) Claims 5 and 15

In addition, dependent Claims 5 and 15 are not taught or suggested by the cited references. Dependent Claims 5 and 15 recite that the information regarding an account for the user in the token includes a new user flag. The Official Action cites the Microsoft Press reference as disclosing Claims 5 and 15, as the reference includes a definition for "flag," which is defined as code that can be embedded in data that identifies some condition or an event of some type. However, as described above with respect to independent Claims 1, 11, 21, and 22, a new user flag is included within the fields of the token, and if the remote server software is set to enable adding new users, the remote server tests to see if a new user account should be established. Although the Microsoft Press reference discloses a flag, none of the cited references teach or suggest providing information regarding an account for the user in the authentication token that includes a new user flag.

(c) Claims 6 and 16

Similarly, it follows that none of the cited references teach or suggest a new user account created by a remote server in response to the new user flag, as recited by dependent Claims 6 and 16. The Official Action cites the Kung '594 patent and the Microsoft Press reference with respect to dependent Claims 6 and 16. The Kung '594 patent only discloses registering a user at a multiple logon server, while the Microsoft Press reference does not disclose creating a new user account at all. Thus, none of the cited references teach or suggest creating a new user account by a remote server in response to a new user flag.

(d) Claims 7 and 17

None of the cited references teach or suggest that the information regarding an account for the user in the token includes user profile update information, as recited by dependent Claims 7 and 17. As described above, the user profile information of the present application may include information about the user that may help the remote server provide efficient service to the user. Thus, in the context of a travel reservation and booking service, the user profile information could be dietary choices, seating preferences, travel spending limits, and other information specific to a given user. Figure 9 of the present application indicates that new or updated user profile information may be contained in the token and transmitted to the remote server. The Official Action cites the Kung '594 patent with reference to registering a user, and the Microsoft Press reference with respect to the definition of "flag." However, none of the references, alone or in combination, teach or suggest a token containing user profile information that is capable of being transmitted to a remote server and updated if needed.

(e) Claims 8 and 18

It follows that none of the cited references teach or suggest updating a user profile with the remote server in response to user profile update information, as recited by dependent Claims 8 and 18. Again with respect to Figure 9 of the present application, after the user profile information is transmitted to the remote server, the remote server determines whether the user is a new user. If the user is new, a new user profile is created, while if the user is not new, the user's profile is updated with the user profile information. However, none of the cited references, alone or in combination, teach or suggest maintaining or creating a user profile to help the remote server provide efficient server to the user, let alone creating or updating the user's profile information.

Therefore, the method, systems, and computer-readable medium of dependent Claims 2-10 and 12-20 are not taught or suggested by the cited references, taken either individually or in combination, for at least the reasons described above. Thus, the rejection of Claims 2-10 and 12-20 under 35 U.S.C. § 103(a) is also overcome.

CONCLUSION

For the above reasons, it is submitted that the final rejection of Claims 1-22 is erroneous and reversal of the rejection is respectfully requested. An Appendix containing a copy of claims involved in the appeal is attached.

Respectfully submitted,

Trent A. Kirk
Registration No. 54,223

CUSTOMER NO. 00826
ALSTON & BIRD LLP
Bank of America Plaza
101 South Tryon Street, Suite 4000
Charlotte, NC 28280-4000
Tel Charlotte Office (704) 444-1000
Fax Charlotte Office (704) 444-1111

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to:
Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450,
on October 6, 2004.

Lorna Morehead
Lorna Morehead

APPENDIX

Claims on Appeal

1. (Previously Presented) A method of performing multiple user authentications with a single sign-on, comprising:

performing a first user authentication;

selecting a remote server subsequent to said first authentication;

sending a token to said remote server containing authentication information responsive to said first authentication, wherein the token also contains information regarding an account for the user including at least one of a new account for the user and an update to an existing account for the user; and

decoding said authentication information, wherein said decoding said authentication information induces a second user authentication.

2. (Original) The method of claim 1, wherein said sending includes sending said token within a universal resource locator.

3. (Original) The method of claim 2, wherein said token includes a timestamp.

4. (Original) The method of claim 2, wherein said token is encrypted.

5. (Previously Presented) The method of claim 1, wherein the information regarding an account for the user in said token includes a new user flag.

6. (Original) The method of claim 5, wherein said remote server creates a new user account in response to said new user flag.

7. (Previously Presented) The method of claim 1, wherein the information regarding an account for the user in said token includes user profile update information.

8. (Original) The method of claim 7, wherein said remote server updates a user profile in response to said user profile update information.

9. (Original) The method of claim 1, wherein said first user authentication occurs within an Intranet.

10. (Original) The method of claim 1, wherein said second user authentication occurs within said remote server.

11. (Previously Presented) A system for performing multiple user authentications with a single sign-on, comprising:

a user sign-on interface, configured to perform a first user authentication;

a link interface, configured to select a remote server subsequent to said first user authentication;

a token configured to be sent to said remote server, said token containing authentication information responsive to said first user authentication and information regarding an account for the user including at least one of a new account for the user and an update to an existing account for the user; and

a decoder configured to decode said authentication information, said decoder further configured to induce a second user authentication.

12. (Original) The system of claim 11, wherein said token is coupled to a uniform resource locator.

13. (Original) The system of claim 12, wherein said token includes a timestamp.

14. (Original) The system of claim 12, wherein said token is encrypted.

15. (Previously Presented) The system of claim 11, wherein the information regarding an account for the user in said token includes a new user flag.

16. (Original) The system of claim 15, wherein said remote server creates a new user account in response to said new user flag.

17. (Previously Presented) The system of claim 11, wherein the information regarding an account for the user in said token includes user profile update information.

18. (Original) The system of claim 17, wherein said remote server updates a user profile in response to said user profile update information.

19. (Original) The system of claim 11, wherein said first user authentication occurs within an Intranet.

20. (Original) The system of claim 11, wherein said second user authentication occurs within said remote server.

21. (Previously Presented) A system for performing multiple user authentications with a single sign-on, comprising:

means for performing a first user authentication;

means for selecting a remote server subsequent to said first authentication;

means for sending a token to said remote server containing authentication information responsive to said first authentication and information regarding an account for the user including at least one of a new account for the user and an update to an existing account for the user; and means for decoding said authentication information, wherein said means for decoding said authentication information induces a second user authentication.

22. (Previously Presented) A machine-readable medium having stored thereon instructions for performing multiple user authentications with a single sign-on, which, when executed by a set of processors, cause said set of processors to perform the following:

performing a first user authentication;

selecting a remote server subsequent to said first authentication;

sending a token to said remote server containing authentication information responsive to said first authentication and information regarding an account for the user including at least one of a new account for the user and an update to an existing account for the user; and

decoding said authentication information, wherein said decoding said authentication information induces a second user authentication.